International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

Implementation of Secure Sharing of PHR's with IoMT Cloud

Swatee S. Nikam, Jyoti P. Kshirsagar

Abstract*: Healthcare area have been introduced to cloud services. The broad acknowledgment of these services in the healthcare area has achieved useful and supportive exchange of Personal Health Records (PHR's). Keeping the information related to health of any individual into cloud servers is vulnerable to disclosure or burglary and requires the enhanced methods that ensure the security of this information. Here we are implementing a methodology for first securing the information and then sharing the same in the cloud, we have also implemented the same with help of using IoMT. This scheme not only guarantees access of control to individuals who are patients where data is stored on the PHR's but also makes use of latest technology to read data of patients with IoMT devices. The patients store the encoded PHR's on the cloud servers and explicitly give access to distinct segments of PHR's to diverse sorts of people other than patient himself. The system includes the use of IoMT (Internet of Medical Things) to capture the live data of patient through WSN (Wireless Sensor Network). This data is encrypted with help of Java Libraries to give encryption at IoT end only thus providing security with IoMT data.

Index Terms*: Health Care Services, IoMT, IoT, Privacy, Security, Encryption.

I. INTRODUCTION

During recent times Internet has penetrated in our everyday life. Many things have revolutionized the way we manage our lives. Internet of things (IoT) tops this list. IoT the vast network of connected things and people, enable users to collect and analyze data through the use of connected devices. Medical equipment used in this advanced technology also see internet integration. Such equipment used with internet of things are termed as Internet of Medical things (IOMT). The Internet of Medical Things (IoMT) is virtually the collection of medical devices and applications that connect to healthcare IT systems through online computer networks. Body Network Sensors are used to bring in live data from patients and stored in PHR.

In addition, cloud-based services help for in this computing where we can access data with any large quantity. Cloud serves as organized storage to vast data and offer access to specific data when and where it is required. For Healthcare data users, such as, patients, hospital staff, specialists, nursing staff, pharmacies, and clinical lab faculty, insurance providers, and the service providers, Cloud serves to guarantee security and privacy. Various techniques have been utilized to guarantee the security of the health-related information stored on the cloud. We propose method for secure PHR's of patient and give control to be managed by them. The strategy saves the classification of the PHR's by limiting the unauthorized users.

The patient himself who is owner of PHR can upload the data related to his health on cloud. This data is uploaded in encrypted form. The patient can decide who and where the data can be used and can share the same with other people. These people might include hospital staff and other people like health insurance company. The patient can limit segments of data to be shared with other people with help of giving restricted usage to people.

II. PROPOSED METHODOLOGY

Methodology proposes an approach that grants patients to regulate the sharing of their own PHR's. The methodology utilizes the two cryptographic methods to guarantee the PHR security. First cryptographic method is used at IoMT end while other at cloud end where two cryptographic algorithms are used for comparing speed based on file upload for PHR. This gives level two authentication and security to every PHR. Further distribution of same PHR is done to give more security by keeping data on different cloud with help of DROPS algorithm.

A. Internet of Medical Things (IoMT)

IoMT includes small remote sensors that are inserted inside or surface mounted on the body of a patient. These sensors constantly monitor the vital physiology parameters of the patient, for example, body temperature beat rate and furthermore monitor the saline level. collected individual health information is aggregated and transmitted through a remote interface, for example, Bluetooth or WLAN. Encryption is done on collected data before it comes to server. This ensures security of data as level 1 security.

B. Personal Health Record (PHR)

Every individual keeps their data on Personal Health record (PHR). This data when given authorization by owner, can be shared with users of data such as Doctors, nursing staff and insurance company. Every data user has a lot of characteristics, for example, alliance,

Manuscript published on 30 September 2019
* Correspondence Author
Ms. Swatee S. Nikam*, Department of Computer Engineering, JSPM's RSCOE, Thatwade, Pune, INDIA.
Ms. Jyoti P. Kshirsagar, Department of Computer Engineering, JSPM's RSCOE, Thatwade, Pune, INDIA.

and sort of hospital services staff, and is approved to look on encoded PHR's dependent on his set of properties. The secret keys are sent to the general public cloud by remote channel and recovered PHR documents are returned. At that point, the data user decrypts the PHR records and confirms the accuracy of decoding.

C. Public Cloud

The Public Cloud has practically boundless storage and computing capacity. This is to embrace the PHR remote storage assignment and react on information recovery request. Lightweight test algorithm is structured in this framework to enhance performance.

D. Key Generation Center (KGC)

KGC creates open parameters for the whole system and distributes secret keys to data users. A data user, set of qualities is inserted in his secret key to acknowledge access control. If the traitor sells his secret key for financial profit, the KGC can trace the character of the malicious user and revoke his secret key.

III. SYSTEM ARCHITECTURE

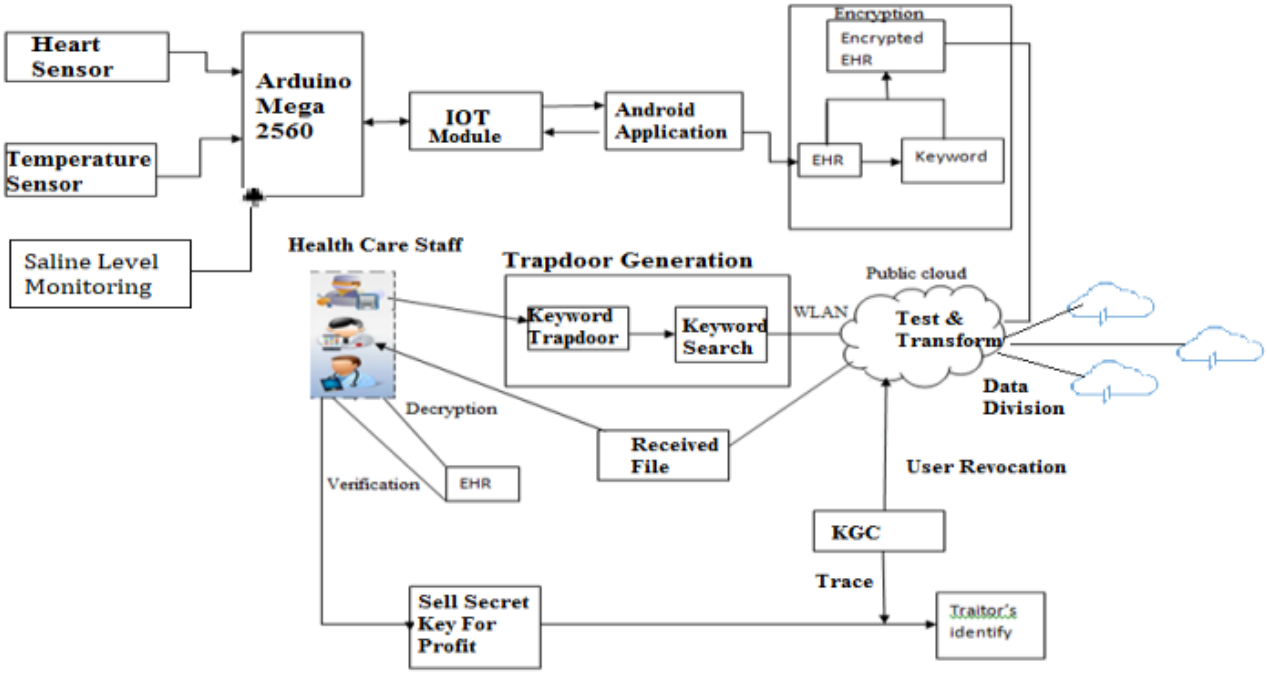

Fig 1: System Architecture

IV. ALGORITHMS

A. Algorithm 1: Advanced Encryption Standard (AES)

We made use of AES algorithm after comparing the same with DES algorithm in implementation. We used AES algorithm in Java libraries first at IoMT end where data which is coming from live sensors is encrypted further it is used in before transferring data to cloud.

Below figure shows steps used in algorithm.

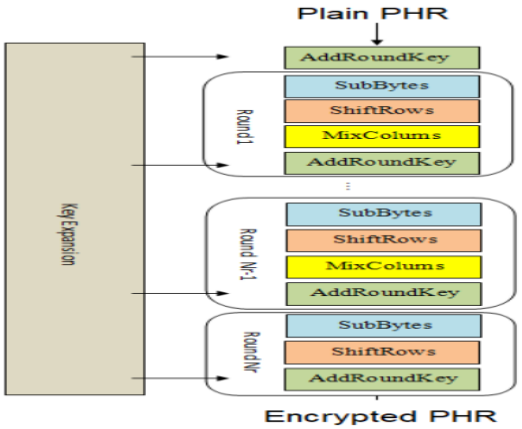

Fig 2: AES Algorithm

B. Algorithm 2: Data in the Cloud for Optimal Performance and Security (DROPS)

Fig 3: Flowchart DROPS

PHR is taken as input File which is then broken into fragments or chunks for level 2 of security.

IV. IMPLEMENTATION AND RESULT

A. Implementation

Fig 4: Registration of PHR Owner

Fig 5: PHR Owner Login

Fig 6 : Create PHR

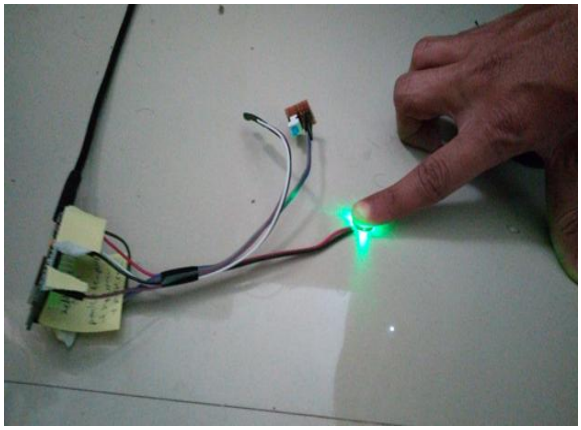

Fig 7: Collecting Data from Sensors

B. Result

1)Algorithmic Analysis:

DES (Data Encryption Standard) and AES (Advanced Encryption Standard) algorithms are analyzed on the bases of time parameter with different file sizes, on machine1 (Intel I3 2.4 GHz Processor with 4 GB RAM). The time taken by the DES and AES security algorithm on the system, using entropy is shown in the following graph. DES algorithm takes more time than the AES algorithm.

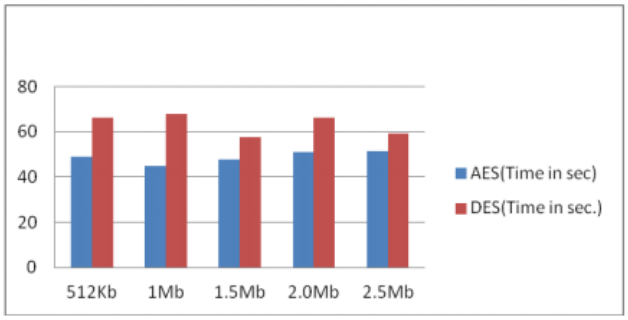

Fig 8: Analysis of Algorithms

2) File Uploading Result:

In the proposed system, storage of data is done on clouds. Before uploading files on the cloud, files are encrypted and then they are stored on the cloud. While storing files on the cloud, it takes some time to write files on the cloud. In our development, we have considered the evaluation time for file upload. File size is in kb(kilobyte), as the file size increases, required time for uploading increases exponentially.

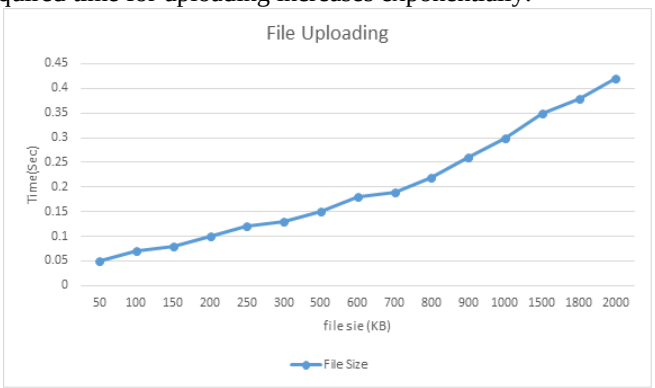

Fig 9: File Uploading Result

V. CONCLUSION

The proposed system is a strategy where data is taken from IoMT sensors, it is secured through encryption and again secured while storing and transmitting the PHR's to the cloud. The technique gives double security to the PHR's and authorizes only authorized person have access to control different parts of the PHR's on the access given by the patients. The activity of the semi-trusted authority is to deliver and store public/private key sets for the data-users in the framework. The performance evaluation is done dependent on the time required to generate keys, encryption, decryption and turnaround time.

REFERENCES

1. Jin-cui YANG, Bin-xing FANG,Security model and key technologies for the Internet of things, The Journal of China Universities of Posts and Telecommunications ,Volume 18, Supplement 2,2011,Pages 109-112, ISSN 1005-8885,https://doi.org/10.1016/S1005-8885(10)60159-8
2. Lo-Yao Yeh, Woei-Jiunn Tsaur, and Hsin-Han Huang. 2017. Secure IoT-Based, Incentive-Aware Emergency Personnel Dispatching Scheme with Weighted Fine-Grained Access Control. *ACM Trans. Intell. Syst. Technol.* 9, 1, Article 10 (September 2017), 23 pages. DOI: https://doi.org/10.1145/3063716
3. Fei Hu, Security and Privacy in Internet of Things (IoT). Models Algorithms and Implementarions, CRC Press, 2016.
4. Arjona, R.; Prada-Delgado, M.Á.; Arcenegui, J.; Baturone, I. A PUF- and Biometric-Based Lightweight Hardware Solution to Increase Security at Sensor Nodes. *Sensors* **2018**, *18*, 2429.
5. S. Venugopalan," Attribute Based Cryptology," PhD Dissertation Indian Institute Of Technology Madras, April-2011.
6. Sumitra B, Pethuru CR & Misbahuddin M, "A survey of cloud authentication attacks and solution approaches", International journal of innovative research in computer and communication engineering, Vol.2, No.10, (2014), pp.6245-6253.
7. Sankar Mukherjee, G.P. Biswas,Networking for IoT and applications using existing communication technology,Egyptian Informatics Journal,Volume 19,Issue 2,2018,Pages 107-127,ISSN 1110-8665,https://doi.org/10.1016/j.eij.2017.11.002.
8. https://www.controlcase.com/services/log-monitoring/
9. Babar, Sachin & Stango, Antonietta & Prasad, Neeli & Sen, Jaydip & Prasad, Ramjee. (2011). Proposed Embedded Security Framework for Internet of Things (IoT). 10.1109/WIRELESSVITAE.2011.5940923.
10. Weber, Rolf. (2010). Internet of Things – New security and privacy challenges. Computer Law & Security Review. 26. 23-30. 10.1016/j.clsr.2009.11.008.
11. K. Zhao and L. Ge, "A Survey on the Internet of Things Security," 2013 Ninth International Conference on Computational Intelligence and Security(CIS), Emeishan 614201, China China, 2013, pp. 663-667. doi:10.1109/CIS.2013.145.
12. **DOI:16.10089.IJMTE.2019.V9I5.19.28046**

AUTHORS PROFILE

Ms. Swatee S. Nikam pursued Bachelor of Engineering in year 2004 from D.Y. Patil College of Engineering & Technology, Kolhapur. She is currently pursuing Master's from JSPM'RSCOE, Thatwade, Pune, India. She has worked in fields of Education and Health. She is working in field of Healthcare with IoT and Network Security as main focus of work. She has 3 years' experience in teaching and 5 years' experience in corporate company

Prof. Jyoti P. Kshirsagar has pursued her Bachelar of engineering in year 2004 from TPCT's COE,Osmanabad She has completed her Masters in Engineering from SCOE,Vadgaon,Punee.She is working as assistant professor at JSPM's RSCOE, Thatwade ,Pune ,India. She is working in field of Image Processing with Machine Laerning and Python as focus of work.